KR Maritime Cyber Safety News & Report

Vol. 051
July. 2022

Korean Register
www.krs.co.kr

CONTENTS

IACS UR E26 & E27 - "Cyber Resilience of ships" Technical Seminar

KR held a technical seminar related to UR E26 & E27, which is the International Association of Classification Societies (IACS)'s Unified Requirement(UR) for Ship Cybersecurity Resilience, on July 5-7, 2022.

The IACS UR E26 & E27 technical seminar was held at the request of customers. In consideration of the recent rapid spread of COVID-19, we visited the customer`s site and related personnel and design engineers attended. The main contents of this technical seminar are as follows.

UR E26 : Cyber resilience of ships

UR E26 is a unified requirement for the implementation of cyber resilience in the ship design and construction, and deals with five aspects: Identify, Protect, Detect, Respond, and Recover. This will be applied to ships contracted for construction on or after 1 January 2024.

Identify (4.1)
- Inventory of CBSs and networks onboard

Protect (4.2)
- Security Zones
- Network protection safeguards
- Antivirus, antimalware, antispam and other protections from malicious code
- Access control
- Wireless Communication
- Remote access control and communication with untrusted networks
- Use of Mobile and Portable Devices

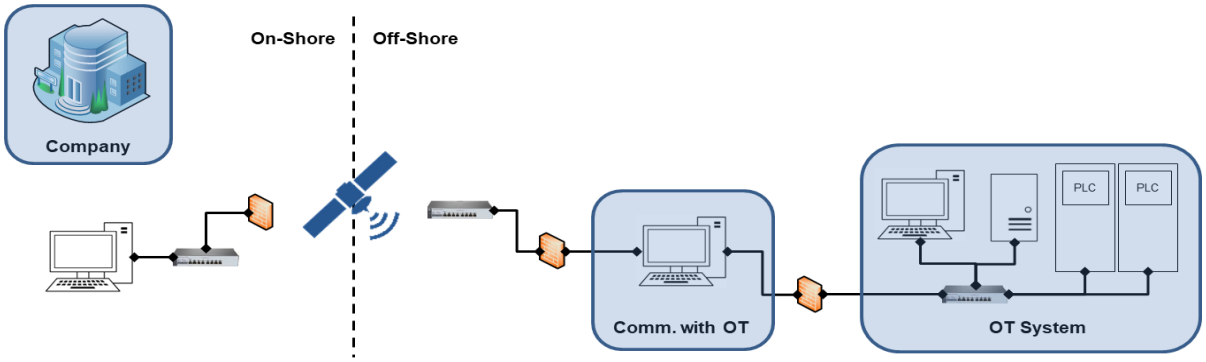
Detect (4.3)
- Network operation monitoring
- Diagnostic functions of CBS and networks

Respond (4.4)
- Incident response plan
- Local, independent and/or manual operation
- Network isolation
- Fallback to a minimal risk condition

Recovery (4.5)
- Recovery plan
- Backup and restore capability
- Controlled shutdown, reset, roll-back and restart

UR E27 : Cyber resilience of on-board systems and equipment

UR E27 is the cyber resilience of ships' onboard systems and equipment, and applies to category II and category III computer-based systems within the scope of UR E26. This UR consists of requirements for cyber resilience of onboard systems and equipment and requirements for Secure Product development Life Cycle (SDLC) required by manufacturers in product development and manufacturing process.



KR will continue to provide technical seminars upon request from customers in the future, and will also provide customized training services for customers who want more detailed training.

* Customized training Q&A : KR Academy Business Team (academy@krs.co.kr)

Maritime Cybersecurity News Scrap

Cyber-attacks on Port of Los Angeles have doubled since pandemic

Source : bbc.com

Cyber-attacks on one of the world's busiest ports have nearly doubled since the start of the Covid pandemic. The number of monthly attacks targeting the Port of Los Angeles is now around 40 million, the port's executive director Gene Seroka told. Los Angeles is the busiest port in the western hemisphere, handling more than $250bn (£210bn) of cargo every year. The threats are believed to come mainly from Europe and Russia, and aim to disrupt the US economy. He said "Our intelligence shows the threats are coming from Russia and parts of Europe. We have to stay steps ahead of those who want to hurt international commerce,"

Working with the FBI

The Port of Los Angeles Cyber Operations Security Centre, operating since 2015 is part of an overall network of FBI cyber watch programs. In addition to that the Port of Los Angeles has invested millions, analyse and share information with those who operate on the dock, such as cargo handlers of dollars in cyber-protection. The Cyber Resilience Centre provides enhanced intelligence gathering and heightened protection against cyber-threats within the maritime supply chain. It is a hub for the port to receiveand shipping lines.

Supply chain blockage

During the pandemic global supply chains slowed down as lockdowns closed factories and workers were forced to stay at home. The strain on supply chains has since eased. In January 2022 there were 109 container ships queuing for more than two days to get into the Port of Los Angeles. Today there are around 20 waiting to dock. But Mr Seroka believes the blockages won't clear completely until 2023. "There's so much cargo coming in and not enough space," he said. "The past two years have proven the vital role that ports hold to our nation's critical infrastructure, supply chains and economy. It's paramount we keep the systems as secure as possible," he added.

IACS Recommendation No.171
Cyber risk management into SMS

Editor : Yoo, Jinho, Senior Surveyor, Korean Register

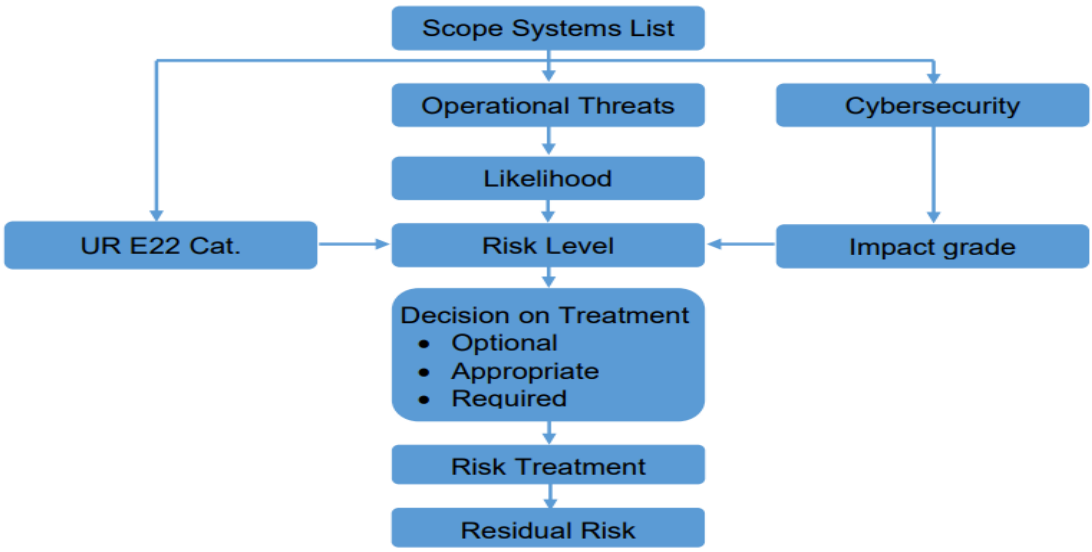
IACS Recommendation No.171 Overview

IACS Recommendation No.171 is a recommendation for integrating cyber risk management into a ship's safety management system (SMS). As the International Maritime Organization (IMO) resolution MSC.428(98) determined that cybersecurity should be addressed in accordance with the existing objectives and functional requirements of the ISM Code, the company (DOC holders) should consider existing safety management systems (and SMS measures)) should be used to assess risks, implement safeguards, and address cybersecurity. This recommendation suggests a risk assessment method to achieve cyber risk assessment for ships owned by the company, and each stakeholder does not necessarily follow this recommendation.

IACS Recommendation No.171 Risk Assessment Methodology

Scope of Application

The risk assessment is applied to a set of IT/OT systems (system list) to be defined. A step-by-step process is then implemented in this list of systems to determine a “risk level” for each system.



IACS Recommendation No.171 Risk Assessment Methodology(Cont.)

Key equipment and technical systems identification

Consider the IACS UR E22 system category for technical systems used in key shipboard operations to identify and evaluate key shipboard operations vulnerable to cyberattacks. System categories are assigned according to their impact on system function.

CATEGORY	CONTENTS
Category I	A system in which the failure of the system does not lead to a hazardous situation for human safety, vessel safety and/or environmental threats.
Category II	System failures can eventually lead to hazardous situations for human safety, vessel safety and/or environmental threats (e.g. Liquid cargo transfer systems, Alarm and monitoring systems, etc.)
Category III	Systems in which a system failure can immediately cause a hazardous situation for human safety, ship safety and/or environmental threats (e.g. Propulsion system, Steering system, etc.)

Impact Assessment

Consider the threat consequences in terms of availability, confidentiality, integrity, and traceability for each system.

IMPACT	DEFINITION	CONTENTS
Impact 1	Negligible	**Events with a negligible impact, such as one or more of the following** - System could be shutdown without any significant effect. - No human or environmental impacts involved.
Impact 2	Acceptable	**Events with an acceptable impact, such as one or more of the following** - shutdown of the system means a pointed disrupt of the service, - environmental impact is in the standard margin and has no consequence but to be declared to authorities, - event could lead to labour disruption because of injuries and medical treatment
Impact 3	Moderate	**Events with moderate impact, such as one or more of the following:** - loss of system activity is significant - disruption of business activity, loss of non-repudiation traceability - loss of confidential information (e.g. data leaks etc.) - human impact leading to permanent disability.
Impact 4	High	**Events with a high impact, such as one or more of the following :** - physical systems damages (e.g. material breakage), - permanent loss of the system - human impact leads to death.
Impact 5	Catastrophic	**Events with a catastrophic impact, such as one of the following:** - physical systems destruction (e.g. fire, explosion), - loss of the vessel (e.g. collision or grounding), - environmental disaster with long-term environmental consequences - human impact leads to multiple deaths or crew, passengers kidnapping.

IACS Recommendation No.171 Risk Assessment Methodology(Cont.)

Likelihood Assessment

1) Human factor (H) calculation

Scores are calculated according to the attacker's level (AT) and the crew's education level (US) as shown in the table below.

	US1	US2	US3	US4
AT5	H2	H3	H3	H4
AT4	H2	H2	H3	H3
AT3	H1	H2	H2	H3
AT2	H1	H1	H2	H2
AT1	H0	H1	H1	H2

AT(Attacker Level)

AT1 : Crew / Unintentional Attacker

AT2 : Crew / Malicious Attacker

AT3 : Standard Attacker

AT4 : Criminal Attacker

AT5 : Cyber warfare Attacker

US(Training /Physical protection / Logical protection)

US1 : High / High / High

US2 : Moderate / High / High

US3 : Low / Moderate / Nothing

US4 : Nothing / Nothing / Nothing

2) Attack Surface (AS) calculation

Scores are calculated according to the degree of connectivity with the outside (CY) and complexity of the internal system (CX) as shown in the table below.

	CY1	CY2	CY3	CY4	CY5
CX3	AS3	AS3	AS4	AS4	AS5
CX2	AS2	AS2	AS3	AS4	AS5
CX1	AS1	AS2	AS3	AS4	AS5

CX(Complexity)

CX1 : Low-maintenance systems

CX2 : Living systems

CX3 : Distributed systems

CY(Connectivity)

CY1 : Isolated System

CY2 : Closed connectivity System

CY3 : Network System

CY4 : DMZ

CY5 : Open Connectivity Systems

IACS Recommendation No.171 Risk Assessment Methodology(Cont.)

3) Probability Index(L) Calculation

Using the attack surface score (AS) and human factor (H) score derived earlier, the probability index is calculated as shown in the table below.

	H0	H1	H2	H3	H4
AS5	L5	L6	L7	L8	L9
AS4	L4	L5	L6	L7	L8
AS3	L3	L4	L5	L6	L7
AS2	L2	L3	L4	L5	L6
AS1	L1	L2	L3	L4	L5

Risk Level Grade assessment

The risk level is determined by the following arithmetic formula according to the previously derived likelihood score, impact score, and UR E22 category grade.

$$2 \times (\text{UR E22 Category} + \text{Probability Likelihood} + \text{Impact} - 4) = \text{Risk Level}$$

Risk Treatment

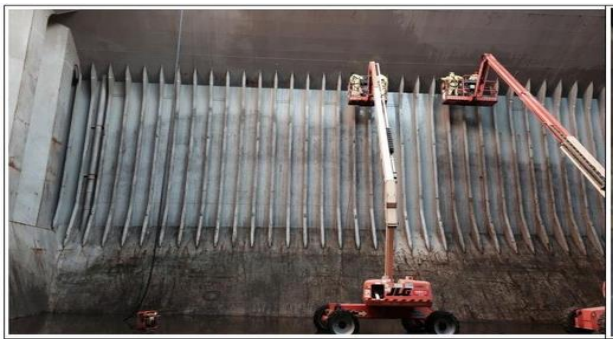
Depending on the risk level rating, responsible cybersecurity and risk mitigation measures may be required depending on the assessment of that layer.

- **RL< 4** : risk treatment is considered "**optional**"
- **4 ≤ RL ≤ 12** : risk treatment is considered "**appropriate**" .
- **RL > 12** : risk treatment is considered "**required**".

The era of remote inspection using drones - Analysis of drone security threats

Editor : Yoo Jinho, Senior Surveyor, Korean Register
Suk Jieon and Son Jinwoo, Korea Maritime & Ocean University

Research on the use of drones in the field of maritime and port is being actively conducted in the world. In the case of ports domain, drones are being used for port surveillance, port security/physical security/patrol, and maritime surveillance. The number of countries using it is gradually increasing. Recently, in ship inspection, remote inspection technology using drones and crawlers (a type that climbs up and down walls) at the same time is being introduced. In the hull inspection of ships, 'precision inspection' and 'thickness measurement' are performed in a way that the inspector directly climbs up and inspects the hull by installing a chief, etc. The remote inspection technology includes a high-level hull inspection using a drone and thickness measurement using a crawler.



<General ship inspection>

<remote inspection using drones>

In addition to ship inspection, as the use of drones increases in many areas, the cyber threats of drones are being announced. Since drones are remotely controlled using a wireless communication network such as WIFI, it is easier to hack than a personal PC or mobile device. There are three main types of drone hacking: spoofing, jamming, and hijacking. The purpose of this study is to examine the case of cyber threats of Drones, and to find out the cyber security requirements to be considered when developing and utilizing services using drones.

Spoofing

Spoofing is a way to send fake data to a drone to make the drone travel or land where the hacker intended. In December 2011, Iran announced that it had forced the US Air Force's state-of-the-art drone RQ-170 Sentinal to land through GPS operation while reconnaissance over Iranian airspace. Iran cut the drone's GPS connection, waited for it to switch to automatic flight mode, and then manipulated it to look for unencrypted GPS frequencies again.

Jamming

Jamming is a method of deliberately radiating, re-radiating, or reflecting electronic signals similar to noise or noise for the purpose of interfering with the enemy's use of electronic equipment, thereby disrupting the enemy's reception. In May 2012, a ‘Camcopter S-100’ manufactured by Schiebel, Austria, crashed during a test flight in Songdo, Incheon, killing one foreign remote pilot and injuring two Koreans. The cause is presumed to be 'GPS reception inability' due to radio wave disturbances in North Korea. The unmanned reconnaissance helicopter that crashed was being introduced by the Navy to monitor the North Korean movement near the Northern Limit Line (NLL) in the West Sea. The police, who investigated the incident, said that during the test flight, the communication and control device in the vehicle that remotely controlled the reconnaissance aircraft malfunctioned, and the autonomous flight system that automatically returned to the original position was activated. considered to have been The company officials who were at the scene also said, "GPS is not working."

Hijacking

Hijacking is a method of illegally hijacking drones that are operating in the same way that terrorists hijack a flying airliner. In 2016, at the security conference ‘2016 PacSec’ held in Tokyo, Japan, they demonstrated the situation of randomly hacking and controlling leisure drones at will. Jonathan Anderson of Tipping Point DV Labs, a research group at security firm Trend Micro, unveiled the Icarus system, which can hack any device that moves with a remote controller, including drones, by taking over communication protocols. This palm-sized device does not simply impede movement through radio wave jamming, but is a 'hacking' method that digs into the security vulnerabilities of the remote control device.

* Source : The Korea JoongAng Daily - Can drones that are easy to hack, can be stolen by disrupting GPS (2018.12)

KR CS++
KR Cybersecurity Training Tool

No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

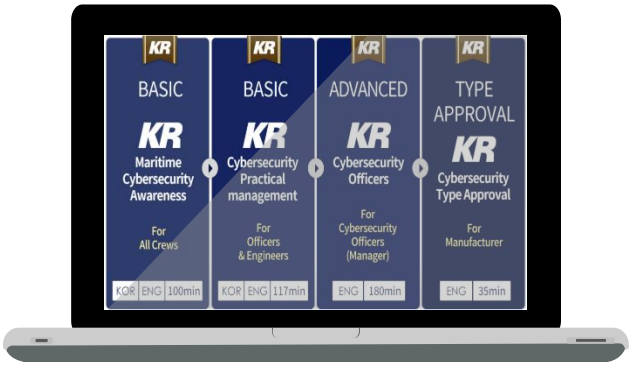
KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.

Online Training

KR Maritime Cybersecurity e-Learning Center training course



Q&A : https://edu.orangecq.com/

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
46762 부산광역시 강서구 명지오션시티 9로 36 (명지동)
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic ok Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr